

REMARKS/ARGUMENTS

Applicants respectfully request reconsideration of the present application in view of the reasons that follow. Claims 1-4, 8, 15-18, 22, 29, 31, and 32 are amended to correct minor typographical errors, to improve clarity, and to remove unnecessary language. Claim 14 has been canceled. Applicants respectfully submit that no new matter has been added. Claims 33-38 were canceled in a prior amendment. After amending the claims as set forth above, Claims 1-13 and 15-32 are now pending in this application.

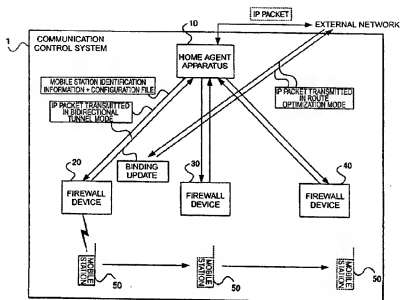
Pending Claims

On the Office Action Summary page, the Examiner indicated that Claims 1-3, 5-17, and 19-32 are pending. Applicants respectfully disagree. In the Office Action mailed on July 16, 2009, the Examiner acknowledged that Claims 1-32 were pending. In the response filed October 7, 2009, the Applicants did not cancel any claims. Claim 14 is canceled herein. As such, it is respectfully submitted that Claims 1-13 and 15-32 are pending in this application. It is also noted that the present Office Action does not address Claims 4 or 18. Applicants respectfully submit that any subsequent Office Action in which Claims 4 or 18 are rejected (based on the newly cited references being used by the Examiner in the present Office Action) should be non-final to provide Applicants with an opportunity to respond to such rejections.

Claim Rejections - 35 USC § 102

On page 2 of the present Office Action, Claims 1-3, 5-17, and 19-32 were rejected under 35 U.S.C. 102(e) as allegedly being anticipated by *Kitahama et al.* (US 2004/0151135). Applicants respectfully traverse the rejection.

In general, *Kitahama et al.* describe a firewall apparatus and method. This firewall method operates by receiving an IP packet from an external network and routing the IP packet to a destination station and, in the opposite direction, it operates by receiving an IP packet from a station and outputting the IP packet to the external network. (See *Kitahama et al.*, para [0054].) As shown below in Fig. 1 of *Kitahama et al.*, data to and from an external network goes via both a “home agent apparatus” and a “firewall device” to a “mobile station.”



In the Office Action, the Examiner points to paragraphs [0056]-[0058] of *Kitahama et al.* as showing the claimed “defining a second address for the interface of the sub-element based on the retrieved identifier of the network element and the first address.” Applicants respectfully disagree with the Examiner’s interpretation.

***Kitahama et al.* does not show “defining a second address for the interface of the sub-element based on the retrieved identifier of the network element and the first address.”**

There is nothing in paragraphs [0056]-[0058] of *Kitahama et al.* that describes “defining a second address for the interface of the sub-element based on the retrieved identifier of the network element and the first address,” as recited in Claim 1. Independent Claims 15 and 29, although of different scope, recite similar elements. Paragraphs [0056]-[0058] are directed to a three step process by which a “firewall ... acquires the destination IP address and source IP address for filtering” of an “IP packet [that] is transmitted ...” (Paragraph [0055]). Paragraphs [0056]-[0058] of *Kitahama et al.* describe the process as follows:

[0056] 1. Where the *IP packet is transmitted in the bidirectional tunnel mode*, i.e., in the case where the source address of the outside IP packet is the home agent address,

where the destination address is a c/o address, and where the IP packet contains an IP packet, *the firewall process 221 acquires the internal IP packet and applies the steps of 2 and 3 below to the IP packet thus acquired.* On the other hand, where the IP packet is transmitted in the other mode than the bidirectional tunnel mode, *the firewall process 221 applies the steps of 2 and 3 below to the original IP packet* acquired from the packet routing part 21.

[0057] 2. Where the IP packet is *transmitted to the mobile station 50 in the route optimization mode*, i.e., in the case where the destination address of the IP packet is a c/o address, where the routing header exists, and where the second destination set in the routing header is a home address, *the firewall process 221 uses the home address as a destination IP address for filtering.* On the other hand, where the IP packet is *transmitted to the mobile station 50 in the other mode than the route optimization mode*, *the firewall process 221 uses the destination address of the IP packet as a destination IP address for filtering* as it is.

[0058] 3. Where the *IP packet is transmitted from a mobile IP terminal in the route optimization mode*, i.e., in the case where the source address of the IP packet is a c/o address and where the home address option is set, *the firewall process 221 uses the address set in the home address option as a source IP address for filtering.* On the other hand, where the *IP packet is transmitted from the mobile IP terminal in the other mode than the route optimization mode*, *the firewall process 221 uses the source address of the IP packet as a source IP address for filtering* as it is.

(Emphasis added).

Thus, paragraph [0056] of *Kitahama et al.* discloses that for transmission of IP packets in the bidirectional tunnel mode, the firewall process acquires an internal IP packet corresponding to the original IP packet and proceeds with steps 2 and 3 described in paragraphs [0057]-[0058]. Paragraph [0056] further discloses that if the transmission is not in the bidirectional tunnel mode that the firewall process applies steps 2 and 3 to the original IP packet (i.e., without acquiring an internal IP packet).

Paragraph [0057], which describes step 2 of the process, discloses that if the IP packet was transmitted *to* the mobile station in the route optimization mode that the firewall process

uses the home address for filtering. Paragraph [0057] further discloses that if the route optimization mode is not used (for IP packets transmitted *to* the mobile station), that the destination address is used for filtering. Paragraph [0058] of *Kitahama et al.*, which describes step 3 of the process, discloses that if the IP packet was transmitted *from* a mobile IP terminal in the route optimization mode, that the firewall process uses the address in the home address field for filtering. Paragraph [0058] further discloses that if the route optimization mode is not used (for IP packets transmitted *from* the mobile terminal), the source address of the IP packet is used for filtering.

Thus, the relied upon portions of *Kitahama et al.* disclose a process for determining which address associated with an IP packet to use for filtering based on the mode used for transmission of the IP packet. *Kitahama et al.* also disclose that the addresses associated with the IP packet can be a home address, a source address, and a destination address. Conversely, Claim 1 recites “**defining a second address for the interface** of the sub-element **based on the retrieved identifier of the network element and the first address.**” (Emphasis added). Applicants respectfully submit that determining which address of an IP packet to use for firewall filtering (as disclosed by *Kitahama et al.*) is not the same as “defining a second address ... based on the retrieved identifier of the network element and the first address,” as claimed. Further, the home address, source address, and destination address disclosed by *Kitahama et al.* are not the same as the claimed “second address.” *Kitahama et al.* fail to teach, suggest, or describe that any of the home, source, or destination addresses are defined “based on the retrieved identifier of the network element and the first address,” as claimed.

The relied-upon portions of *Kitahama et al.* (and elsewhere) fail to teach, suggest, or describe at least “a second address” or “defining” of “a second address,” as claimed. It follows that the relied-upon portions of *Kitahama et al.* (and elsewhere) also fail to teach, suggest, or describe at least “defining a second address” “based on the retrieved identifier of the network element and the first address,” as claimed. (Emphasis added). Such features are simply not present in *Kitahama et al.* If the Examiner maintains the rejection, Applicants respectfully request that the Examiner explain in detail how *Kitahama et al.* is alleged to disclose such elements.

A rejection under 35 U.S.C. 102(e) cannot be properly maintained where the reference does not teach each and every element of the claim. For at least these reasons, Applicants respectfully request withdrawal of the rejection of independent Claims 1, 15, and 29. For at least the same reasons, Applicants respectfully request withdrawal of the rejection of dependent Claims 2, 3, 5-14, 16, 17, 19-28, and 30-32.

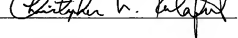
Applicants believe that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by the credit card payment instructions in EFS-Web being incorrect or absent, resulting in a rejected or incorrect credit card transaction, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicants hereby petition for such extension under 37 C.F.R. §1.136 and authorize payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date April 19, 2010

By: 

FOLEY & LARDNER LLP
Customer Number: 23524
Telephone: (608) 258-4286
Facsimile: (608) 258-4258

Christopher L. Kalafut
Attorney for Applicant
Registration No. 57,946